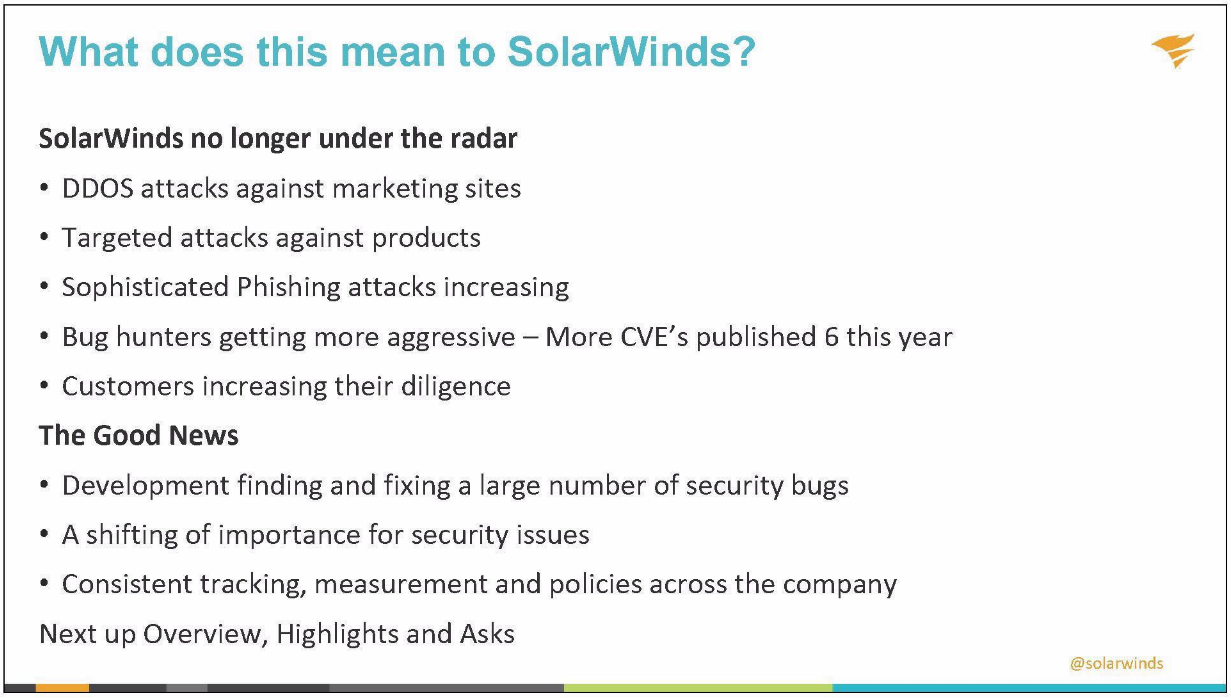
Exhibit 50

Excerpts of SW-SEC00006628

solarwinds

PM Security Vulnerability & Incident Review

July 10, 2020



What does this mean to SolarWinds?

SolarWinds no longer under the radar

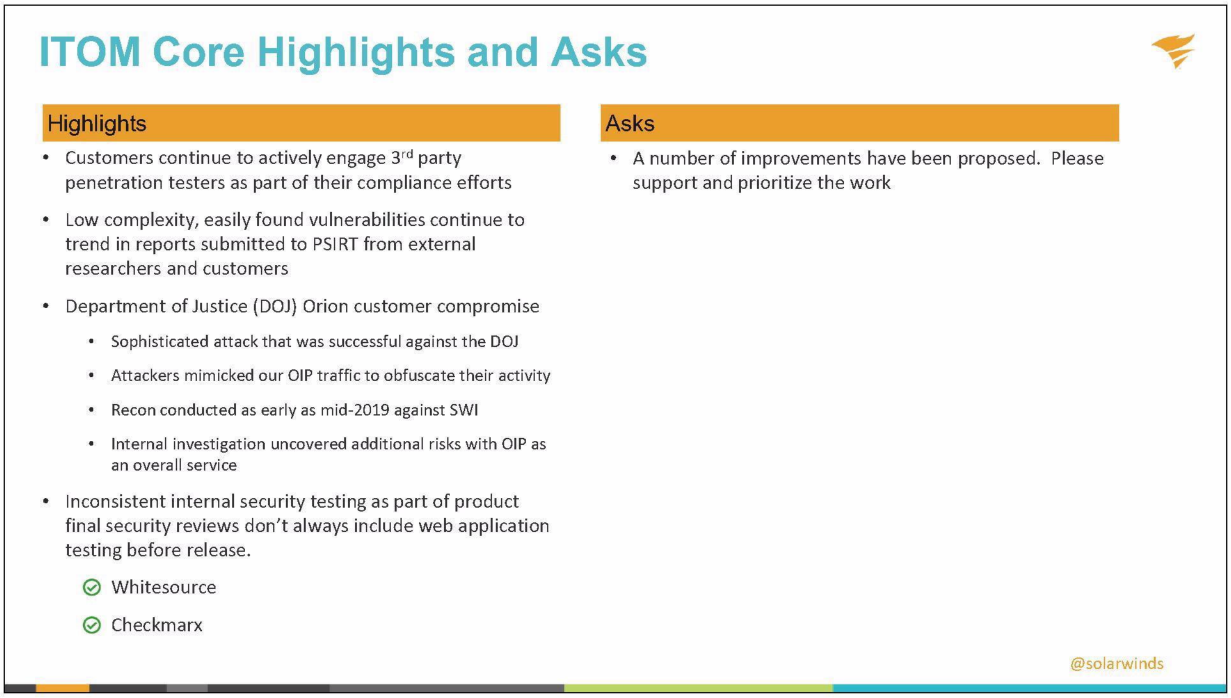
- DDOS attacks against marketing sites
- Targeted attacks against products
- Sophisticated Phishing attacks increasing
- Bug hunters getting more aggressive – More CVE’s published 6 this year
- Customers increasing their diligence

The Good News

- Development finding and fixing a large number of security bugs
- A shifting of importance for security issues
- Consistent tracking, measurement and policies across the company

Next up Overview, Highlights and Asks

@solarwinds



ITOM Core Highlights and Asks

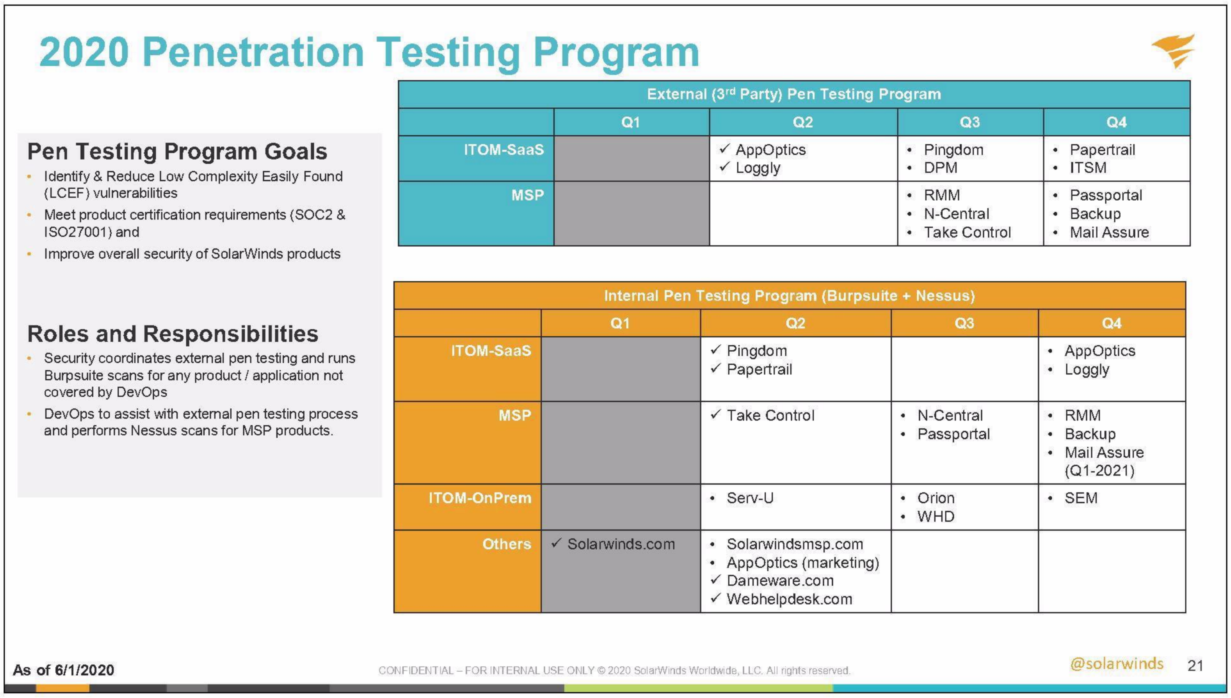
Highlights

- Customers continue to actively engage 3rd party penetration testers as part of their compliance efforts
- Low complexity, easily found vulnerabilities continue to trend in reports submitted to PSIRT from external researchers and customers
- Department of Justice (DOJ) Orion customer compromise
  - Sophisticated attack that was successful against the DOJ
  - Attackers mimicked our OIP traffic to obfuscate their activity
  - Recon conducted as early as mid-2019 against SWI
  - Internal investigation uncovered additional risks with OIP as an overall service
- Inconsistent internal security testing as part of product final security reviews don’t always include web application testing before release.
  - ✓ Whitesource
  - ✓ Checkmarx

Asks

- A number of improvements have been proposed. Please support and prioritize the work

@solarwinds



2020 Penetration Testing Program

Pen Testing Program Goals

- Identify & Reduce Low Complexity Easily Found (LCEF) vulnerabilities
- Meet product certification requirements (SOC2 & ISO27001) and
- Improve overall security of SolarWinds products

Roles and Responsibilities

- Security coordinates external pen testing and runs Burpsuite scans for any product / application not covered by DevOps
- DevOps to assist with external pen testing process and performs Nessus scans for MSP products.

External (3rd Party) Pen Testing Program

	Q1	Q2	Q3	Q4
ITOM-SaaS		✓ AppOptics ✓ Loggly	• Pingdom • DPM	• Papertrail • ITSM
MSP			• RMM • N-Central • Take Control	• Passportal • Backup • Mail Assure

Internal Pen Testing Program (Burpsuite + Nessus)

	Q1	Q2	Q3	Q4
ITOM-SaaS		✓ Pingdom ✓ Papertrail		• AppOptics • Loggly
MSP		✓ Take Control	• N-Central • Passportal	• RMM • Backup • Mail Assure (Q1-2021)
ITOM-OnPrem		• Serv-U	• Orion • WHD	• SEM
Others	✓ Solarwinds.com	• Solarwindsmsp.com • AppOptics (marketing) ✓ Dameware.com ✓ Webhelpdesk.com		

As of 6/1/2020

@solarwinds 21

On Prem
Orion has been done pen testing of products – need to align on reporting.
NPM, SCM, should be included.

Consistent on scanning policies and reporting
InfoSec: Consistent coverage across the pen testing program.

MSP – security assessments against product itself – Unknown? Similar to Burpsuite.

Make a clear requirement, by when and in what scenarios.